VULNERABILITY BULLETINS

Patches Released for Vulnerabilities Affecting VMware Products

TLP:WHITE

Sep 18, 2024

Broadcom released an advisory (VMSA-2024-0019) to address a pair of vulnerabilities affecting VMware vCenter Server and VMware Cloud Foundation.

The first vulnerability, tracked as CVE-2024-38812, is the most severe of the two. It is a heap overflow security flaw in vCenter's Distributed Computing Environment/Remote Procedure Call (DCERPC) protocol implementation, in which an adversary can send a maliciously crafted packet to execute remote code.

The second vulnerability, tracked as CVE-2024-38813, is a privilege escalation vulnerability that could allow an adversary to elevate privileges to root by sending a similar type of crafted network packet.

Successful exploitation of both vulnerabilities requires an adversary to gain network access to vCenter Server in order to trigger the security flaws.

Affected Products:

- VMware vCenter Server
  - Versions 8.0 and 7.0

- VMware Cloud Foundation
    - Versions 5.x and 4.x

Health-ISAC provides this information for situational awareness and encourages users to upgrade affected product versions.

Recommendations:

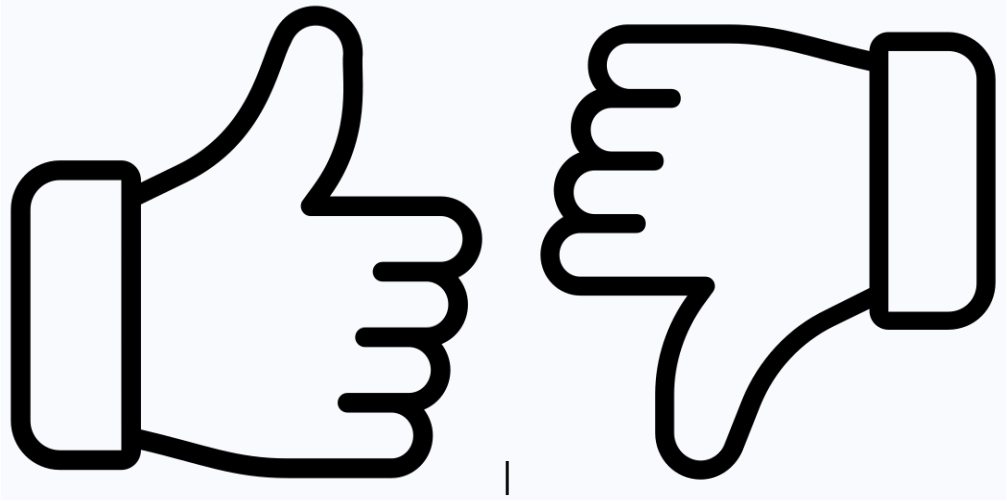
- Apply the available patch for affected versions.
- Monitor systems and logs for any suspicious or unauthorized activity.
- Ensure incident response plans are frequently tailored to address security breaches effectively.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Broadcom, Bleeping Computer, Security Online, Security Week, The Register, The Hacker News, Help Net Security

Alert ID f7c7080a

View Alert

Share Feedback
was this helpful?



Tags CVE-2024-38813, CVE-2024-38812, VMware Cloud Foundation, VMware vCenter Server

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**